Web Images
 Maps
 News
 Shopping
 Gmail
 more ▼
 Sign in

 Google
 group homomorphism undeniable signature
 Search Peterences

Web Books Results 1 - 10 of about 453 for group homomorphism undeniable signature. (0.34 seconds)

Progress in Cryptology Mycrypt 2005: First ... - Google Books Result by Edward Dewson, Serge Vaudenay - 2005 - Computers - 329 pages An undeniable signature scheme therefore consists of a key setup algorithm and a ... this scheme to the more general framework of group homomorphisms [13]. ... books. google.com/books/sib=mc840299390...

Method to generate, verify and deny an undeniable signature invention Title: Method to generate, verify and deny an undeniable signature Abstract: applying to each block (xi) a group homomorphism (f) to obtain a resulting ... www.freshpatents.com/Method-to-generate-venty-and-deny-an-undeniable-signaturedirectospoyl or branzo(050 193048,pth - 28k - Cached - Similar pages

(WO/2005/081451) METHOD TO GENERATE, VERIFY AND DENY AN UNDENIABLE ... The method according to claim 2, wherein the group homomorphism (f) computation is ... A Method of confirming by a Verifier an undeniable signature (v1, ... www.wipo.in/pctdb/en/wo.jsp?iA=EP2005001335&DISPLAY=CLAIMS - 30k - Cached - Smilar pages

port Optimization of the MOVA Undeniable Signature Scheme File Format PDFAdobe Acrobat - View as HTML this undeniable signature scheme. First, let us recall some basic definitions from [13] related to the interpolation. of group homomorphisms. Definition 1.... www.monnerat.info/abilications/posimization.odf - Simiter pages

Thèse EPFL 3691 (2006) Jean Monnerat

On the other hand, by selecting group homomorphisms with a small group range ... Based on these protocols, we devise our new undeniable signature scheme and ... library.epil.ch/theses//nr=5691 - 33k - Cached - Similar pages

Vaudenay: Undeniable Signatures Based on Characters: How to Sign... We introduce a new undeniable signature scheme which is existentially ... proposed at Asiacrypt '04 which is based on a secret group homomorphism... citeseerx.ist.psu.edu/showciting/jeessionde=/1F2FD10C86A79C8E7FF925531680442? cite_3467039 -21k - Cached - Similar page.

Advances in Cryptology, ASIACRYPT 2004: 10th ... - Google Books Result by Pil Joong Lee - 2004 - Computers - 548 pages (15), all previous undenlable signatures were based on the discrete ... 2 The Group Homomorphism Interpolation Problem 2.1 Problem Definitions Given two ... books.google.com/books/19bbn=3540283758 ...

LNCS 3329 - Generic Homomorphic Undeniable Signatures the sense that we transform a private group homomorphism from public, groups G to H (the order of H being public) into an undeniable signature, scheme. ... www.spingerlink.com/index/480/K2P4L7GJB9ALX.pdf - Similar pages

Scientific Commons: Optimization of the MOVA Undeniable Signature ...
Optimization of the MOVA Undeniable Signature Scheme (2007) ... its generalization proposed at Asiacrypt'04 which is based on a secret group homomorphism. ...
en.scientificcommons.org/22465151 . 94 . Cachied - Similar pages

| POFT Generic Homomorphic Undeniable Signatures
| File Format: PDF/dobe Acrobat - View as HTML
Interpolation of Group Homomorphisms. Our Signature Scheme. Conclusion. Generic
Homomorphic Undeniable Signatures. J. Monnerat. S. Vaudenay ...
www.inis.re.kr/ac04/data/Asiacrypt/2004/09%20Digital%20Signatures/01_Jean%
20Monneraturf - Similar Dagee

4	2	3	4	5	6	7	Ω	a	10	Next

ρ......

group homomorphism undeniable signature Search

 $Search\ within\ results\ |\ Language\ Tools\ |\ Search\ Tips\ |\ Dissatisfied?\ Help\ us\ improve\ |\ Try\ Google\ Experimental\ Properties of the propert$



Home | Login | Logard | Acases Information | Alerts | Precision Her

Welcome United States Palent and Trademark Office

BROWSE

SEARCH

HEER XPLORE GUIDE

Educational Courses

Results for "(('group homomorphism')<in>metadata)"

Your search matched 3 of 1803509 documents,

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.



« Search Ophons

View Session History

New Search

- Key

IE EE CAF

REEF INL IEEE Journal or Magazine IEY JNI. IET Journal or Magazine

IEEE Conference Proceeding

ETCNE IET Conference Proceeding

IERE STD IEEE Standard Mugay Seeran (('group homomorphism')<in>metadata) Saurea N Check to search only within this results set

Displey Format Citation Citation & Abstract

Interactive online content developed from IEEE conference tutorials.

view selected items

IEEE/IET

Select All Deserect All

Books

1. Perturbations in optimal trellis source code design Kieffer, J.:

information Theory, 2005, ISIT 2005, Proceedings, International Symposium on 4-9 Sept. 2005 Page(s):1927 - 1931

Digital Object Identifier 10.1109/ISIT.2005.1523681 AbstractPlus | Full Text: PDF(223 KB) IEEE CAF

Rights and Permissions 2. A characterization of 1-perfect additive codes

Borges, J.; Rifa, J.; Information Theory, IEEE Transactions on Volume 45, Issue 5, July 1999 Page(s):1688 - 1697

Digital Object Identifier 10.1109/18.771247 AbstractPlus | Beferences | Full Text: PDE(364 KB) 1666 UNL

Rights and Permissions

3. Algorithms for matrix groups and the Tits alternative Beals, R.:

Foundations of Computer Science, 1995. Proceedings, 36th Annual Symposium on

23-25 Oct. 1995 Page(s):593 - 602 Digital Object Identifier 10.1109/SFCS.1995.492589

AbstractPlus | Full Text: PDF(868 KB) HEEE CNF

Rights and Permissions

Help Contec @ Ones





Subscribe (Full Service) Register (Limited Service, Free) Login.

Search: The ACM Digital Library The Guide

Found

THE ACM DIGITAL LIBRARY

"aroup homomorphism"

Feedback

Terms used: group homomorphism

Save results to a Binder

Refine these results with Advar Search

Sort results by Display results

relevance expanded form

Open results in a new window

Try this search in The ACM Gui

Results 1 - 7 of 7

Learning Equivariant Functions with Matrix Valued Kernels Marco Reisert, Hans Burkhardt

Ade by GON

October 2007 The Journal of Machine Learning Research, Volume 8 Publisher: MIT Press

Full text available: pdf(410.57 KB) Additional Information: full citation, abstract, index terms

Online Jo Full-text ic academic Questia C www.Cus-ein

Bibliometrics: Downloads (6 Weeks): 4. Downloads (12 Months): 26. Citation Count: 0 This paper presents a new class of matrix valued kernels that are ideally suited to learn vector valued equivariant functions. Matrix valued kernels are a natural

generalization of the common notion of a kernel. We set the theoretical foundations of ...

10 Rules

Signature of symmetric rational matrices and the unitary dual of lie groups Jeffrey Adams, B. David Saunders, Zhendong Wan

Fat Lose 9 lbs Days By f 10 Idiot R www.Fall.com

July 2005 ISSAC '05: Proceedings of the 2005 international symposium on Symbolic and algebraic computation

Publisher: ACM

Full text available: pdf(215.88 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 19, Citation Count: 0 A key step in the computation of the unitary dual of a Lie group is the determination if certain rational symmetric matrices are positive semi-definite. The size of some of the computations dictates that high performance integer matrix computations be ...

Dynamic Filling Append, s secure m PDF & mo

Keywords: lie group, matrix signature, symmetric matrix

warm active F

3 Learning Equivariant Functions with Matrix Valued Kernels

Marco Reisert, Hans Burkhardt

May 2007 The Journal of Machine Learning Research, Volume 8 Publisher: MIT Press

Journal F Find Jour 3000 Sou Out For F gover Higheig

Full text available: Todf(410.54 KB) Additional Information; full citation, abstract, references, index ferms

Bibliometrics: Downloads (6 Weeks): 1. Downloads (12 Months): 48. Citation Count: 0

This paper presents a new class of matrix valued kernels that are ideally suited to learn vector valued equivariant functions. Matrix valued kernels are a natural

generalization of the common notion of a kernel. We set the theoretical foundations of

4 Smooth invariant interpolation of rotations

F. C. Park, Bahram Ravani
July 1997 ACM Transactions on Graphics (TOG), Volume 16 Issue 3 Publisher: ACM

Full text available: pdf(561.24 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 101, Citation Count: 9 We present an algorithm for generating a twice-differentiable curve on the rotation group SO(3) that interpolated a given ordered set of rotation matrices at their specified knot times. In our approach we regard SO(3) as a Lie group with a biinvariant ...

Keywords: Lie algebra, Lie group, cubic spline, interpolation, mathematics, rotation

5 Quantum mechanical algorithms for the nonabelian hidden subgroup problem Michelangelo Grigni, Leonard Schulman, Monica Vazirani. Umesh Vazirani

July 2001 STOC '01: Proceedings of the thirty-third annual ACM symposium on Theory of computing

Publisher: ACM

Full text available: Doff: 174.83 KB) Additional Information: full citation, abstract, references, cited by,

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 21, Citation Count: 16 We provide positive and negative results concerning the "standard method" of identifying a hidden subgroup of a nonabelian group using a quantum computer.

6 On the completeness of object-creating database transformation languages

Jan Van Den Bussche, Dirk Van Gucht, Marc Andries, Marc Gyssens March 1997 Journal of the ACM (JACM), Volume 44 Issue 2 Publisher: ACM

Full text available: notified a Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 65, Citation Count: 2 Object-oriented applications of database systems require database transformations invologing nonstandard functionalities such as set manipulation and object creation. that is, the introduction of new domain elements. To deal with thee functionalities, ...

Keywords: computational completeness, constructive transformation, first-order logic, object creation, object-oriented database, while loop

7 A data structure for a uniform approach to computations with finite groups

Max Neunhöffer, Ákos Seress July 2006 ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation

Publisher: ACM

Full text available: Top pdf(192.09 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 17, Citation Count: 0 We describe a recursive data structure for the uniform handling of permutation groups and matrix groups. This data structure allows the switching between permutation and matrix representations of segments of the input group, and has wide-ranging applications. ...

Keywords: GAP, black-box group, computational group theory, constructive membership, large-base group, matrix group algorithm, permutation group algorithm

Results 1 - 7 of 7

The ACM Portal is published by the Association for Computing Machinery, Copyright @ 2008 ACM, Inc. Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

Web Images Maps News Shopping Gmail more. Sign in

Google

"group homomorphism" signature

Search Advanced Search Petersices

Web Books Results 11 - 20 of about 5.490 for "group homomorphism" signature. (0.22 seconds)

IPDFJ Verifiable Encryption and Applications to Group Signatures and ... File Format. PDF/Adobe Acrobat - View as HTML that you know a signature on given message reduces to demonstrating that you. know a preimage under a group homomorphism. This is true for any of the stan-... www.brinsd.kfm2/98/5/6/6/5-8-8-8-3-2 ddf - Smillar peaces

IPDFI Factorization-based Fail-Stop-Signature Schemes Revisited File Format: PDF/Adobe Acrobat - View as HTML Forgery of Ordinary Digital Signature Schemes. K. Schmidt-Samoa h is a group homomorphism. The bundling degree of h equals p. K. Schmidt-Samoa www.informatik.u-darmstatche/KPstaffkafa/cios04.pd- Smillar pages

Vaudenay: Undeniable Signatures Based on Characters: How to Sign ... We introduce a new undeniable signature scheme which is existentially ... proposed at Asiacryt 104 which is based on a secret group homomorphism. ... citeseerx.ist.psu.edu/showciting/jsessionid=425A0439FAE638508C8FABCF959C11E? cite_3467039 - 21k - Cazche-1 Smiliar pages

Homomorphic Signature Schemes

In a series of talks, Rivest suggested the investigation of homomorphic signa-, ture schemes. For instance, the RSA signature scheme is a group homomorphism.
www.springerlink.com/index/HFPVUTVEGWYK36PC.pdf - Similar pages

PlanetMath: signature of a permutation

is called the signature or sign of the permutation \$ g\$. ... This is version 6 of signature of a permutation, born on 2003-02-26, modified 2004-10-31. This is version 6 of signature of a planetmath.org/encytopedia/SignatureOfAPermutation.html - 32k - Cached - Similar pages

[PS] A REMARK ON A SIGNATURE SCHEME WHERE FORGERY CAN BE PROVED File Format: Adobe PostScript - View as Text

A new type of signature scheme, a signature scheme where forgery by an Since g is a group-homomorphism, each z ∈ im(g) ⊆ G has the same number of ... www.semper.org/sirene/pub/EIPW 91FSS-Homo Ecr90.s.gz - Similar pages

Springer Online Reference Works

The signature of an algebraic system is the collection of relations and ... of degree and if for each the mapping defines a group homomorphism from lo own springer.de/IS/s085060.htm - 37k - Cached - Similar pages

Topics in Cryptology, CT-RSA 2002: The Cryptographers' Track at ... - Google Books Result by Ban Preneel - 2002 - Computers - 509 pages If we have a multiplicative signature scheme Sigx : G → R as well as a group homomorphism <f1 : Z/mZ → G from the additive group Z/mZ to the ... books.google.com/books/sibh=354V43248...

Epkenhans: An analogue of Pfister's local-global principle in the ... These signature homomorphisms correspond to signatures of the Witt ring. ... Then HNIK is well-defined as a group homomorphism since 1 > -< < (N <) > ... pib.oadram.org/inb-bin/fitem?d=JTNB_1999_11_1_31_0 · Similar pages

Method to generate, verify and deny an undeniable signature ...
The above described group homomorphism of the undeniable signature scheme is in the context of characters to hard characters, which means a nontrivial ...

www.ireapatehsonline.com/v205/6193048.html - 86k - Cached - Sumiar pages

Previous 1 2 3 4 5 6 7 8 9 1011 Next

"group homomorphism" signature

Search

Search within results | Language Tools | Search Tips | Try Google Experimental

Web Images Maps News Shopping Gmail more v Sian in Google Advanced Search group homomorphism Search Preferences Web

Results 1 - 10 of about 188,000 for group homomorphism. (0.26 seconds)

Group homomorphism - Wikipedia, the free encyclopedia

Image of a Group homomorphism(h) from G(left) to H(right). The smaller oval inside H is the image of h. N is the kernel of h and aN is a coset of h. ...

en.wikipedia.org/wiki/Group_homomorphism - 31k - Cached - Similar pages

Homomorphism - Wikipedia, the free encyclopedia Even though the set may be the same, the same function might be a homomorphism, say, in group theory (sets with a single operation) but not in ring theory ... en.wikipedia.org/wiki/Homomorphism - 35k - Cached - Similar pages More results from en wikipedia.org »

Group Homomorphism -- from Wolfram MathWorld

A group homomorphism is a map f:G->H between two groups such that the group ... Hence, any (nontrivial) homomorphism from a simple group must be injective. ... rnathworld.wolfram.com/GroupHomomorphism.html - 20k - Cached - Similar pages

ABSTRACT ALGEBRA: OnLine Study Guide, Section 3.7

Let μ: G1 -> G2 be a group homomorphism. Then G1/μ is isomorphic to μ(G1). ... There are many important examples of group homomorphisms that are not ... www.math.niu.edu/~beachv/abstract_algebra/study_guide/37.html - 12k -Cached - Similar pages

ABSTRACT ALGEBRA ON LINE: Groups (part 2)

Proposition If: G1 -> G2 is a group homomorphism, then ... (Homomorphisms defined on cyclic groups) Let C be a cyclic group, denoted multiplicatively, ... www.math.niu.edu/~beachy/agol/groups2.html - 12k - Cached - Similar pages

PlanetMath: group homomorphism

A composition of group homomorphisms is again a homomorphism. ... This is version 22 of group homomorphism, born on 2001-11-08, modified 2006-10-16. ... planetmath.org/encyclopedia/GroupHomomorphism.html - 28k - Cached - Similar pages

PlanetMath: group homomorphism

Oct 16, 2006 ... A group homomorphism is a function \$\phi\colon G \to K\$ such that \$\phi\(s) \ast t) = \phi(s) \ for all \$s,t \in G\$

planetmath.org/encyclopedia/EndomorphismOfAGroup.html - 28k - Cached - Similar pages More results from planetmath org -

Homomorphisms and Isomorphisms

Math reference, group homomorphisms and isomorphisms. ... That's it; that's all we need for a group homomorphism, homomorphism from Z to Z mod 7 ... www.mathreference.com/grp,homo.html - 6k - Cached - Similar pages

frefl 38 Group Homomorphisms

A group homomorphism is a mapping from one group to another that respects multiplication and inverses. They are implemented as a special class of mappings, ... www.pap-system.org/Manuals/doc/htm/ref/CHAP038.htm - 44k - Cached - Similar pages.

History of Mathematics Blog » Blog Archive » Group homomorphism Group homomorphism. February 28, 2008 - 9:13 pm ... Reload this page in a moment. is a homomorphism from a finite group G onto G' and that G' has an element ... histmath net/2008/02/28/group-homomorphism/ - 12k - Cached - Similar pages

2	3	4	5	6	7	Α	Q	10	Next

group homomorphism	Search	
Search within results Language Tools Search Tips	Dissatisfied? Help us improve	Try Google Experimental
***************************************		***************************************

Web Images Maps News Shopping Gmail more • Sign in Google group homomorphism abelian group Search Preferences

Web Results 1 - 10 of about 723,000 for group homomorphism abelian group. (0.29 seconds)

Group homomorphism - Wikipedia, the free encyclopedia if G and H are abelian (i.e. commutative) groups, then the set Hom(G, H) of all group homomorphisms from G to H is itself an abelian group; the sum h + k of ... en.wikipedia.org/wiki/Group_homomorphism - 31k - Cached - Similar pages

Abelian group - Wikipedia, the free encyclopedia (This is not true if H is a non-abelian group.) The set Hom(G, H) of all group homomorphisms from 6 to H thus turns into an abelian group in its own right. ... en.wikipedia.org/wiki/Abelian_group - 43k - Cached - Similar pages More results from en.wikipedia.org >

JSTOR: The First Derived Equaliser of a Pair of Abelian Group.... In this note We attack the problem of classifying a pair of abelian group homomorphisms by introducing a con-struction which we call "the derived... links jator.org/stof?sict=0002-9939(197401)42%3A1%3C77%3ATFDEOA%3E2.0.CO%3B2-U--Similar.page.

Commutative Semigroups with Group-Homomorphism § 1. Introduction ... homomorphism gl of S into an abelian group Gl having the universal. repelling property with respect to homomorphisms from S into abelian. groups. ... joi.jio.jst.go.jp/JST_Journalarchive/pjab 1945/47.871*Prom=Google - Similar pages

PlanetMath: abelian group

Oct 15, 2003 ... Theorem ĭ Any subgroup of an abelian group is normal. Proof. Let \$ H\$... If such a function were a homomorphism, we would have ... planetmath.org/encyclopedia/AbelianGroup2.html - 29k - Cached - Similar pages

[PDF] 1 abelian group 266 absolute value 307 addition mod P 427 additive ... File Format: PDF/Adobe Acrobat - View as HTML

abelian group 266, absolute value 307, addition mod P 427 ..., group 183, 266, 293, group homomorphism 355, group of permutations 47, group of units 293 ... www.math.unn.edu/-garrett/cryptofindex.pdf - Similar pages

A Universal Complete Metric Abelian Group of a Given Weight by ... A Universal Complete Metric Abelian Group of a Given Weight ... a quotient mapping which is a group homomorphism) of G onto H. Furthermore we prove that, ... at yorku.ca/ba/bi/o/02.htm - 3k - Cached - Similar pages

ECCC Report TR08-020 and related Papers

Mar 7, 2008 ... Decodability of Group Homomorphisms beyond the Johnson Bound ... and thus codes derived from homomorphisms over abelian groups may be viewed ... ecc. hot-web de/eccc-reports/2008/TR08-020/index.html - 4k - Gached - Sumilar pages

Abelian Group Theory papers of Andreas R. Blass
Let G be an abelian group and let k be the smallest rank of any group whose direct sum ...
all its homomorphisms to Z factor through finite subproducts. ...
www.math.lsa.umich.edu/~abiass/abga.html - 13k - Cached - Sunillar pages

ABSTRACT ALGEBRA ON LINE: Groups (part 2)

Since any vector space is an abelian group under vector addition, any linear transformation

between vector spaces is a group homomorphism. ... www.math.niu.edu/~beachy/aaol/groups2.html - 12k - Cached - Similar pages

1 2 3 4 5 6 7 8 9 10 Next

group homomorphism abelian group Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve | Try Google Experimental



Indexed by

Help Contac

O Carr

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

THE ACM DIGITAL LIBRARY

Feedback

"group homomorphism" and signature
Terms used: group homomorphism signature

Found 1 of

Sort results relevance

Save results to a Binder

Refine these results with Advance Search

by
Display expanded form
Open results in a new window

Try this search in The ACM Guide

Results 1 - 1 of 1

results

Signature of symmetric rational matrices and the unitary dual of lie groups
Jeffrey Adams, B. David Saunders, Zhendong Wan

Ass by Google

July 2005 ISSAC 05: Proceedings of the 2005 international symposium on Symbolic and algebraic computation
Publisher: ACM

Full text available: pdf(215.88 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 19, Citation Count: 0

A key step in the computation of the unitary dual of a Lie group is the determination if certain rational symmetric matrices are positive semi-definite. The size of some of the computations dictates that high performance integer matrix computations be ...

Keywords: lie group, matrix signature, symmetric matrix

Software Deve Tool 20X Faster, Au Software Build Download Free

Software Build-Download Free Whitepapers. Blechlo-Cloud com

Requirements
Management
Agile Software
Development N
Download You
User Version.

Software for S Thinkwise Soft Factory Award development to

Doing Require Finally! A know based tool BAs to define 360° Results 1 - 1 of 1

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player